Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Bauten und Logistik BBL
Projektmanagement / Fachberatung
Technisches Gebäudemanagement / Domotik

Weisungen zu den Standards für Zutrittskontrollsysteme (ZUKO)

01.02.2026

Das Bundesamt für Bauten und Logistik (BBL) erlässt folgende Weisungen:

Inhaltsverzeichnis

1 Zweck und Geltungsbereich 4

1.1 Ziel der Weisung 4
1.2 Geltungsbereich 4
1.3 Abweichungen zur Weisung 4
1.4 Abgrenzung bestehende Systeme 4

2 Glossar 5

3 Grundsätze Zutrittskontrollanlage (ZUKO) 6

3.1 Definition 6
3.2 Anwendungsbereich 6
3.3 Gesetzliche Grundlagen und Weisungen 6
3.4 Bestand der Zutrittskontrollsysteme 7
3.5 Anbindung zur Einbruchmeldeanlage (EMA) 8
3.5.1 Vorgaben BBL 8
3.5.2 Zuständigkeiten 8

3.6 Rollen und Aufgaben 10
3.6.1 Fachberatung Sicherheit 10
3.6.2 TGM-Domotik 10
3.6.3 Projektmanagement (PM) 10
3.6.4 Objektbewirtschaftung- und Betrieb (OBB) 10
3.6.5 Planer und Lieferanten 10

4 IKT-Bestimmungen 11

4.1 Allgemein 11
4.2 IKT- Infrastruktur 11
4.2.1 Technik-Architektur 11

4.3 Kommunikationsebene 12
4.3.1 Netzwerk 12
4.3.2 Power over Ethernet (PoE) 12
4.3.3 Zeitserver NTP 12
4.3.4 Spezifikation Patchkabel Kupfer 12

4.4 Einhaltung der IKT-Vorgaben 13
4.4.1 Vulnerability Management 13
4.4.2 Minimum an Zugriffsrechten 13
4.4.3 Technische Härtung 13
4.4.4 Anti-Virus Lösung 13
4.4.5 Einsatz Kryptographie und digitale Zertifikate 13
4.4.6 Network Access Control 14
4.4.7 USB-Geräte 14
4.4.8 LifeCycle Management spezifischer Hilfsprogramme 14
4.4.9 Schliessen von Sicherheitslücken 14
4.4.10 Regelmässige Updates der installierten Software 14
4.4.11 Erstellen eines regelmässigen Abbilds (dump) von Datenbanken 14

5 Managementebene ZUKO-System 15

5.1 Aufbau 15
5.2 Funktionalitäten 15
5.2.1 Mandantenfähigkeit 15
5.2.2 Benutzerverwaltung 15
5.2.3 Anbindung an Datenbezugspunkt Bund 15
5.2.4 Berechtigungskonzept für Mandantenadministratoren 15
5.2.5 Objektverwaltung 15
5.2.6 Zutrittsberechtigungsverwaltung 16
5.2.7 Protokollierung 16
5.2.8 Systemsprachen 16

5.2.9 Reporting ... 16
5.2.10 Testumgebung ... 16
5.3 Bedienung ... 16
5.3.1 Mehrbenutzersystem ... 17
5.4 Systemanforderungen ... 17
5.5 Lizenzierung ... 17
5.6 Fernzugriff und Support ... 17
5.6.1 Datentransfer ... 18
5.6.2 Sorgfaltspflichtserklärung ... 18
6 Automationsebene ZUKO-System ... 19
6.1 Allgemein ... 19
6.2 Adressierungskonzept ... 20
6.3 Schnittstelle Automationsebene zur Managementebene ... 21
6.4 Anbindungen Feldebene ... 21
6.5 Hardware ... 21
6.5.1 Technische Grundlagen ... 21
6.5.2 ZUKO-Controller ... 21
6.5.3 Online-Leser ... 22
6.5.4 Offline-Komponenten ... 22
6.5.5 Validierungsleser ... 22
6.5.6 SAM-Karten (Taufkarten zu Offline-Komponenten) ... 22
6.5.7 Programmer zu Offline-Komponenten ... 22
7 Zutrittsmedium ... 23
7.1 Allgemein ... 23
8 Schulungen ... 23
9 Dokumentation ... 23
9.1 Betriebshandbuch ... 23
9.2 Share Point ... 23
10 Verfasser und Bezugsquelle ... 24
11 Inkraftsetzung ... 24

1 Zweck und Geltungsbereich

1.1 Ziel der Weisung

Mit der vorliegenden Weisung wird der Standard sowie die technischen Spezifikationen und Anforderungen für Zutrittskontrollsysteme definiert.

1.2 Geltungsbereich

Die vorliegende Weisung hat Gültigkeit für alle bestehenden (siehe Kapitel 1.4) und neuen Zutrittskontrollsysteme der zivilen Bundesverwaltung in der Schweiz. Die Weisung muss bei der Planung und Umsetzung eingehalten werden, wenn neue ZUKO-Komponenten oder neue ZUKO-Systeme verbaut werden. Die verantwortliche Organisation beim BBL (Objektmanagement / Projektmanagement) sowie das beauftragte Planungsteam (Sicherheitsfachplaner / Türfachplaner), sowie die beauftragten Unternehmer und Lieferanten sind verpflichtet, die vorliegende Weisungen umzusetzen.

1.3 Abweichungen zur Weisung

Abweichungen zu den in dieser Weisung beschriebenen Spezifikationen und Anforderungen müssen mit der Fachberatung Sicherheit und der TGM-Domotik abgesprochen und vor Ausführungsbeginn genehmigt werden. Bei identifizierten Abweichungen nimmt der Lieferant in erster Instanz mit dem Sicherheitsfachplaner- und als Rückfallebene mit der TGM-Domotik Kontakt auf und informiert vor der Umsetzung.

1.4 Abgrenzung bestehende Systeme

Bestehende Zutrittskontrollsysteme werden grundsätzlich nicht der Weisung entsprechend anpasst.
Hinweis: Bei Erweiterungen, Umbau- oder Modernisierungsprojekten hat die vorliegende Weisung für die betroffenen Systemkomponenten oder das Managementsystem Gültigkeit und muss entsprechend umgesetzt werden.

2 Glossar

Begriff / Abkürzung	Titel
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
BAB	Bundesarbeitsplatz
BBL	Bundesamt für Bauten und Logistik
TGM-Domotik	Team Domotik des Technisches Gebäudemanagement BBL
BIT	Bundesamt für Informatik und Telekommunikation
DMZ	Demilitarized Zone
DSG	Datenschutzgesetz
EMA	Einbruchmeldeanlage
IAM	Identity & Access Management
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnologie
LDAP	Lightweight Directory Access Protocol
NAC	Network Access Control
Nutzer	Berechtigte Personen in der jeweiligen Verwaltungseinheit, welche die Zutrittsrechte vergeben (Mandantenadministrator)
OSS	Open Security Standards
PoE	Power over Ethernet
PoLP	Principle of Least Privilege
RAS	Remote Access Service
SAM	Secure Access Module
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SSL	Secure Socket Layer
TGM	Technisches Gebäudemanagement
VDI	Virtuelle Desktopinfrastruktur
VM	Virtuelle Maschine
ZUKO	Zutrittskontrollsysteme

3 Grundsätze Zutrittskontrollanlage (ZUKO)

3.1 Definition

Der Begriff Zutrittskontrolle vereinigt alle baulichen, technischen und organisatorischen Massnahmen, die einen nicht autorisierten Zutritt zu Anlagen und Objekten einschränken, regeln und/oder verhindern.
Anlagen und Objekte sowie deren Inhalte sind vor unerlaubtem Zutritt und Zugriff zu schützen, Räume organisatorisch zu trennen, Personenströme zu lenken, Personen nötigenfalls zu separieren und zu registrieren.

3.2 Anwendungsbereich

Der Anwendungsbereich und Umfang eines Zutrittskontrollsystems wird objektspezifisch im jeweiligen Sicherheitskonzept definiert. Im Dokument «K0_A2_Anhang zu Handbuch Standards und Leistungsabgrenzung», ist die Grundausstattung eines Objektes beschrieben.

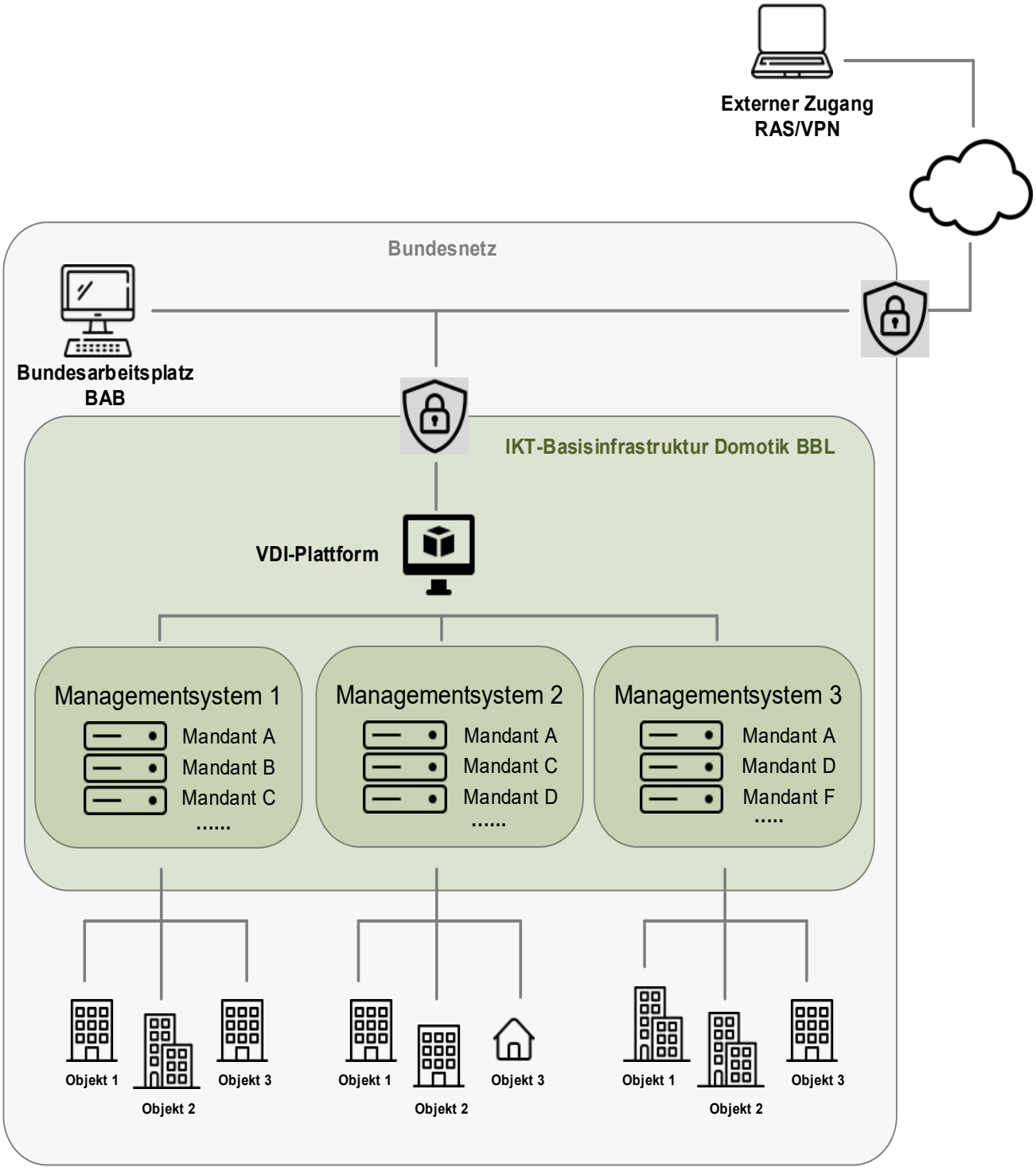
3.3 Gesetzliche Grundlagen und Weisungen

Es gelten mindestens die folgenden Gesetze, Verordnungen und Weisungen:

- Bundesgesetz über den Datenschutz (DSG)
- Verordnung über den Datenschutz (DSV)
- Bundesgesetz über die Informationssicherheit (ISG)
- Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (ISV)
- Si001 – IT-Grundschutz in der Bundesverwaltung
- 209d Weisungen zur Kennzeichnung und Beschriftung von Gebäudetechnik-Installationen
- Weisungen CAD-Daten-BBL

3.4 Bestand der Zutrittskontrollsysteme

Die bestehenden ZUKO der zivilen Bundesverwaltung sind als Campus Lösungen aufgebaut. Ein Campus besteht aus einem Managementsystem, mit einer beliebigen Anzahl Objekte und einer beliebigen Anzahl Mandanten. Für jeden Mandanten werden Rechte- und Zugriffsmöglichkeiten vergeben. Nutzer werden einem Mandanten zugeordnet und erhalten so auf den Managementsystemen die notwendigen Zugriffsrechte auf die ihnen zugeordneten Objekte (siehe Kapitel Funktionalitäten)



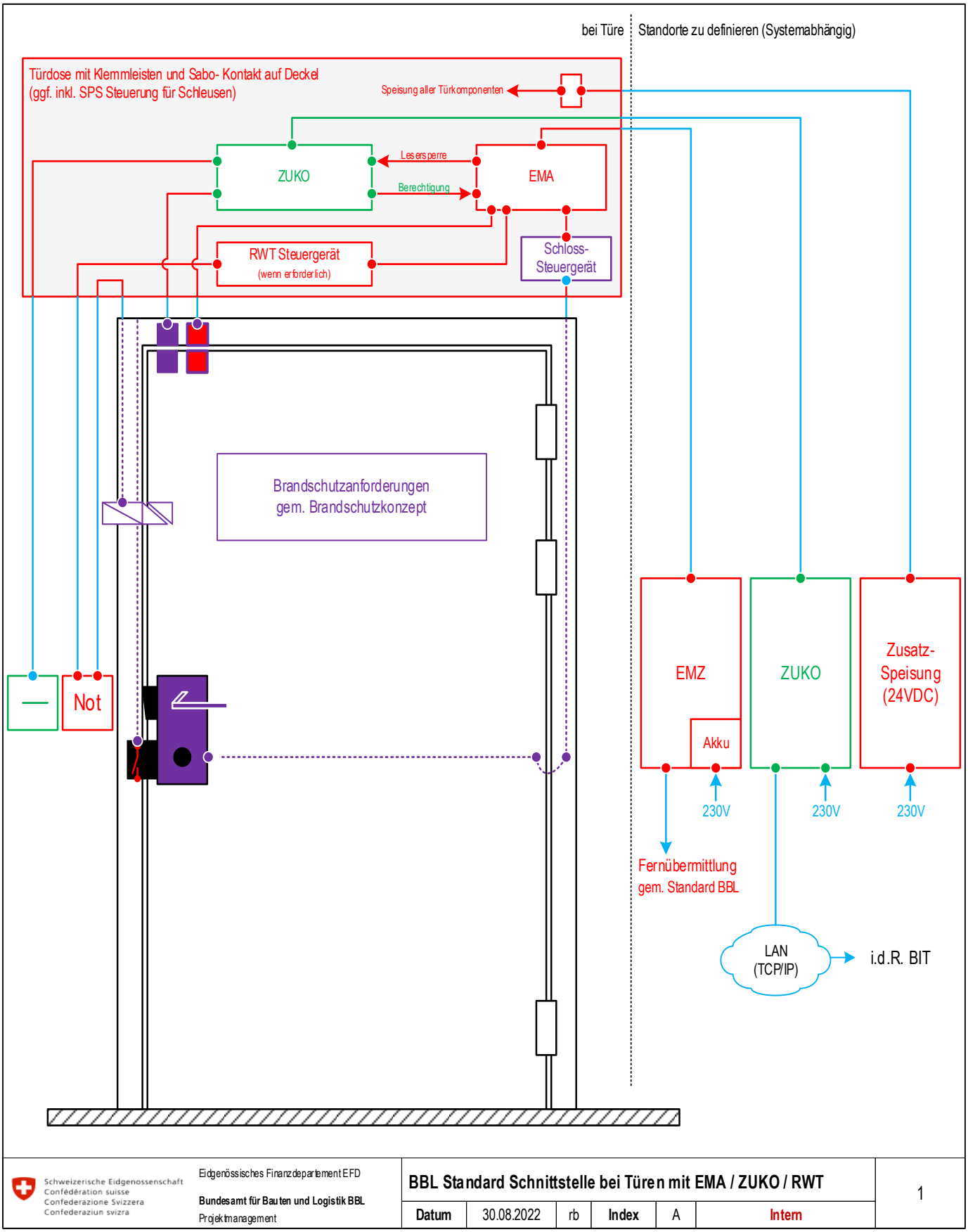
3.5 Anbindung zur Einbruchmeldeanlage (EMA)

3.5.1 Vorgaben BBL

Die nachfolgende Darstellung zeigt die Schnittstellen bei Türen sowie die Zuständigkeiten innerhalb der Gewerke ZUKO, EMA sowie den Einsatz von Rettungswegtechnik. Der Errichter EMA übernimmt in enger Zusammenarbeit mit dem Türbauer und dem Errichter ZUKO den Lead über die erforderlichen Türfunktionen. Diese Vorgaben sind verbindlich einzuhalten, Abweichungen sind nur nach vorhergehender Vereinbarung mit dem BBL zulässig.
Die Speisung aller für die Türfunktion erforderlichen Komponenten (exkl. EMA und Türantriebe) erfolgt ab einer zentralen Speisung (24VDC). Der Errichter EMA konzipiert das entsprechende Speisungskonzept und setzt dieses um. Ausgenommen die Zentrale der EMA sowie deren peripheren Komponenten ist grundsätzlich keine USV erforderlich. Wenn im Objekt eine Notstromversorgung existiert, soll diese nach Koordination mit dem Elektroplaner verwendet werden.

3.5.2 Zuständigkeiten

- Planung, Beschaffung und Umsetzung erfolgt durch die zuständige Projektleitung
- Planung, Beschaffung und Umsetzung erfolgt durch die zuständige Projektleitung gemäss den weiteren Vorgaben des Fachspezialisten bzw. Türfachplaners
- Das Zutrittskontrollsystem gibt das Signal «Berechtigung» an EMA, es hat keine direkte Überwachungsfunktion. Ggf. ist ein Kontakt «Lesersperre» ab EMA entgegenzunehmen
- Die Einbruchmeldeanlage überwacht und steuert die Türe und stellt auch die Funktion der Rettungswegtechnik sicher. Der EMA-Errichter übernimmt den Lead an der Türe.
- Die erforderlichen Elektroinstallationen werden durch den Elektroplaner nach Angabe der Errichter EMA und ZUKO erstellt.



Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	Eidgenössisches Finanzdepartement EFD **Bundesamt für Bauten und Logistik BBL** Projektmanagement	**BBL Standard Schnittstelle bei Türen mit EMA / ZUKO / RWT**				1
		Datum	30.08.2022	rb	**Index** A	**Intern**

3.6 Rollen und Aufgaben

3.6.1 Fachberatung Sicherheit

Die Fachberatung Sicherheit erstellt die BBL-Standards zu den Fachthemen Security und Safety und ist für deren Umsetzung verantwortlich.

3.6.2 TGM-Domotik

Die TGM-Domotik ist verantwortlich für den Betrieb und die IKT-Sicherheit der Zutrittskontrollsysteme (Managementebene). Für die bundesweiten Nutzer der Zutrittskontrollsysteme, betreibt die TGM-Domotik eine moderne und hochverfügbare IKT-Infrastruktur und stellt zusammen mit den Lieferanten die entsprechenden Fachanwendungen bereit.

3.6.3 Projektmanagement (PM)

Ist bei Neubau- und Sanierungsprojekten zuständig, dass die vorliegende Weisung an das Planerteam und/oder an den Sicherheitsplaner übergeben wird. Diese sind verantwortlich, dass die vorliegende Weisung bei allen Vorhaben und Projekten umgesetzt wird.

3.6.4 Objektbewirtschaftung- und Betrieb (OBB)

Ist bei Sanierungsprojekten zuständig, dass die vorliegende Weisung an das Planerteam und/oder an den Sicherheitsplaner übergeben wird. Diese sind verantwortlich, dass die vorliegende Weisung bei allen Vorhaben, Projekten und Sanierungen umgesetzt wird.

3.6.5 Planer und Lieferanten

Sind verantwortlich für die Umsetzung der Weisung bei Vorhaben, Projekten und Sanierungen.

4 IKT-Bestimmungen

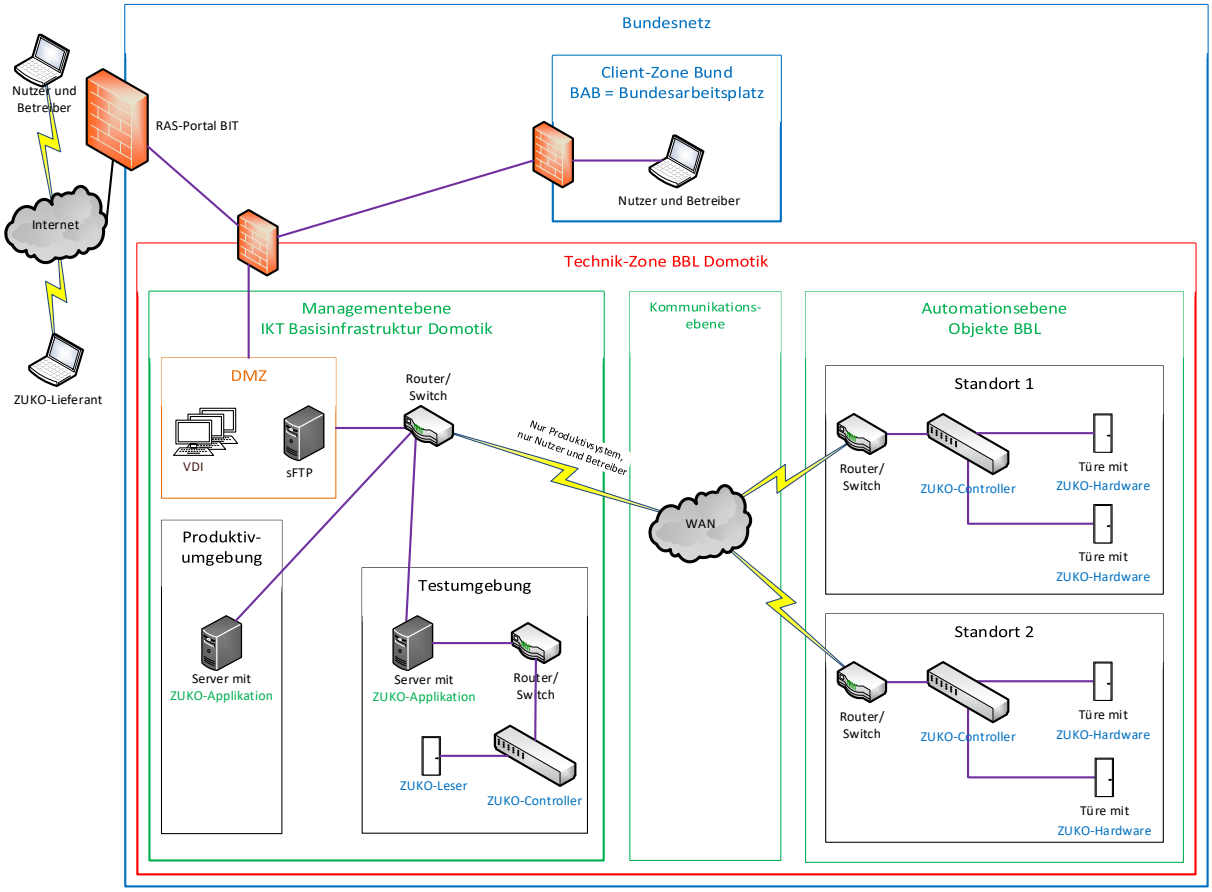
4.1 Allgemein

In diesem Kapitel werden IKT-Richtlinien beschrieben, welche bundesweit Gültigkeit haben.

4.2 IKT- Infrastruktur

4.2.1 Technik-Architektur

Soft- und Hardware befinden sich in der «Technik-Zone BBL Domotik», diese ist Teil des Bundesnetzes.



Betreiber und Nutzer greifen über einen Bundesarbeitsplatz (BAB) oder mit einem VPN-Tunnel aus dem Internet auf die Komponenten der Demilitarized Zone (DMZ) zu. Im zweiten Fall geschieht die Anmeldung über das Portal des Remote Access Service (RAS) des Bundesamts für Informatik und Telekommunikation (BIT).
Server und virtuelle Clients werden bei Campuslösungen von der TGM-Domotik zur Verfügung gestellt und in der «Technik-Zone BBL Domotik» betrieben.

4.3 Kommunikationsebene

4.3.1 Netzwerk

Die Kommunikation erfolgt ausschliesslich über das Netzwerk und Netzwerkkomponenten des BIT.

Dabei gelten folgende Bestimmungen:

- Statische IP-Adressierung: Kein Einsatz dynamischer IP-Adressvergabe (DHCP). Die Vergabe der nötigen IP-Adressen erfolgt, auf Bestellung des ZUKO-Lieferanten, durch die TGM-Domotik des BBL
- Private Netzwerke und Komponenten sind nicht zulässig.
- Realisierung auf IPv4. Neu verbaute Komponenten müssen IPv6 tauglich sein
- On-Premises: Es besteht keine Verbindung zum Internet. Cloud-Produkte sind nicht zulässig. Sämtliche Software- und Hardwareelemente müssen ohne Anbindung an eine Cloud oder das Internet, uneingeschränkt funktionsfähig sein.
- Wireless Anbindungen sind grundsätzlich nicht zugelassen. Sofern eine Wireless Anbindung aus technischen oder baulichen Gründen notwendig ist, muss diese durch die TGM-Domotik genehmigt werden.

4.3.2 Power over Ethernet (PoE)

Bei Bedarf können durch das BIT PoE Ports bereitgestellt werden. Das BIT hat ebenfalls Switches mit PoE / Type 3 / 60W im Einsatz. Der Einsatz von PoE müssen in der Phase 3 (Projekt) zwischen dem Elektroplaner und dem Sicherheitsplaner definiert werden. Der Bedarf von PoE muss dem BBL spätestens mit der Bestellung der IP-Adressen angemeldet werden.

4.3.3 Zeitserver NTP

Für die Synchronisierung der Zeit der einzelnen Komponenten muss der BIT-interne Network Time Protocol (NTP)-Server verwendet werden. Dieser ist bereits bauseitig vorhanden.

4.3.4 Spezifikation Patchkabel Kupfer

Für das BBL-Netzwerk erforderlichen Patchkabel (inkl. Steckerkappen) sind in der Farbe, gemäss untenstehender Tabelle, durch den ZUKO-Lieferanten zu liefern. Die Patchkabel müssen mindestens die folgenden Spezifikationen aufweisen: Steckersystem RJ45, Cat.6_A, S/FTP, AWG26.
Die Patchungen zwischen Switch Port und Feldinstallation werden durch den ZUKO-Lieferanten erstellt und auf der IP-Liste der TGM-Domotik dokumentiert.

Anwendung	Kabelfarbe	Knickschutzfarbe
EMA	Gelb	Blau
Energiemessungen (PDU)	Gelb	Grün
Brand	Gelb	Orange
ZUKO	Gelb	Violett
TNA	Gelb	Rot
SLS (GSA, CCTV)	Gelb	Schwarz
PSA	Gelb	Weiss
IKT H24	Gelb	Grau

4.4 Einhaltung der IKT-Vorgaben

In den folgenden Kapiteln sind die IKT-Vorgaben definiert. Einerseits sind dies die Vorgaben des BBL bezüglich der verwendeten Komponenten und Applikationen. Andererseits sind auf der verlinkten Seite die Informatiksicherheitsvorgaben Bund, sowie unter den Vorgaben des BACS der gültige IT-Grundschutz (Si001 – IT-Grundschutz in der Bundesverwaltung) zu finden.
Wichtiger Grundsatz:
Es sind keine Verbindungen zu externen Netzwerken erlaubt – insbesondere nicht zum Internet. Alle Systeme sind On-Premises zu betreiben und Aktualisierungen müssen innerhalb des BIT-Netzwerks erfolgen.

4.4.1 Vulnerability Management

Jegliche Systeme, welche über IP erreichbar sind, müssen gegen Cyberattacken resilient (sichergestellt durch Sicherheitsupdates, Systemaktualisierung gemäss SLA) sein. Dies bedingt weiter, dass der ZUKO-Lieferant regelmässig und zeitnah Sicherheitsupdates für die einzelnen Systeme über die gesamte Betriebsdauer installiert. Die TGM-Domotik behält sich das Recht vor, Schwachstellen-Scans durchzuführen. Entsprechende Fehler müssen vom ZUKO-Lieferanten gemäss den Vorgaben der TGM-Domotik behoben werden.

4.4.2 Minimum an Zugriffsrechten

Für die Nutzung von Zutrittskontrollsystemen gilt folgendes:
- Es dürften ausschliesslich persönliche Accounts verwendet werden. Nicht benötigte Accounts müssen durch den Lieferanten oder durch die Administratoren, der TGM-Domotik gemeldet werden. Diese werden anschliessend deaktiviert oder gesperrt.
- Die Zugriffskontrolle muss technisch erzwungen werden
- Nicht authentifizierte Zugriffe sind unzulässig
- Die Rollenvergabe erfolgt nach dem Principle of least Privilege (PoLP).

4.4.3 Technische Härtung

Die Systeme müssen nach aktuellem Stand der Technik gehärtet werden, wobei insbesondere folgende Punkte zu beachten sind:
- Nicht benötigte Kommunikationsports, -protokolle, -verbindungen und Schnittstellen sowie Dienste, Anwendungen und Funktionalitäten müssen deaktiviert, gesperrt oder entfernt werden.
- Kein Dual Homing: Dual Homing-Geräte sind nicht erlaubt. Dies hat zur Folge, dass kein IP-fähiges Gerät in mehreren IP-Subnetzen vorhanden ist.
- Die systemeigenen Sicherheitsparameter müssen so konfiguriert werden, dass eine Erhöhung der Systemsicherheit erreicht wird (z.B. Aktivierung von Protokollierung und Alarmierung).
- Anleitungen betreffend Härtung und sichere Konfiguration (sog. Hardening Guidelines) müssen vom Auftragnehmer für alle netzwerkbasierten Komponenten definiert und dokumentiert werden.

4.4.4 Anti-Virus Lösung

Die TGM-Domotik übernimmt das Anti-Virus Management der Betriebssysteme gemäss internen Vorgaben.

4.4.5 Einsatz Kryptographie und digitale Zertifikate

Es werden sicherheitstechnisch starke und sicher konfigurierte kryptographische Algorithmen, Verfahren und Mittel eingesetzt, welche auf einem globalen Kryptographie-Standard basieren. Grundsätzlich werden SSL/TLS-Zertifikate durch die interne Zertifizierungsstelle der TGM-Domotik bereitgestellt. Es sind keine self-signed Zertifikate zugelassen. Falls der Auftragnehmer ein SSL/TLS-Zertifikat benötigt, muss dieses beim BBL (TGM-Domotik) mit einem erstellten Request File bestellt werden. Abschliessend muss das Zertifikat durch den Antragsteller eigenständig integriert werden. Die Gültigkeit der Zertifikate beträgt 3-Jahre.

4.4.6 Network Access Control

Die TGM-Domotik wird künftig Network Access Control (NAC) einsetzen, um die Kontrolle über den Anschluss von Systemen an die lokale Netzwerkinfrastruktur sicherzustellen. Als Anforderung für alle IP-fähigen Geräte gilt jedoch, dass sie das IEEE 802.1x EAP-TLS (zertifikatsbasierte) Protokoll unterstützen.

4.4.7 USB-Geräte

Grundsätzlich sind keine USB-Geräte erlaubt. Falls technisch nicht anders umsetzbar, gilt: Für Geräte (Lizenz Dongles, Smartcard Leser, Programmer, usw.), welche über USB kommunizieren, muss der ZUKO-Lieferant ein Gateway USB/Ethernet, z.B. «Digi Anywhere USB», liefern und in Betrieb setzen bzw. in das Netzwerk einbinden. Der Einsatz solcher Geräte muss in jedem Fall vorgängig mit der TGM-Domotik abgesprochen und koordiniert werden.
Die TGM-Domotik überprüft monatlich, ob bei «Digi Anywhere» Updates vorliegen. Sobald ein relevantes Update zur Verfügung steht, wird dieses durch das BBL (TGM-Domotik) installiert oder es wird der Lieferant für dessen Installation beauftragt.

4.4.8 LifeCycle Management spezifischer Hilfsprogramme

Jegliche Software, welche der Lieferant auf einer VM der Bundesverwaltung installiert, wird durch ihn gepflegt und auf dem aktuellen Stand gehalten. Software, welche jährliche Lizenzkosten generiert, darf nur installiert werden, wenn diese Kosten vorab offeriert und durch das BBL bestellt worden sind. Werden spezifische Peripheriegeräte eingesetzt, fallen auch deren Firmware und Treiber in diesen Aufgabenbereich.

4.4.9 Schliessen von Sicherheitslücken

Der Lieferant identifiziert laufend Schwachstellen und Sicherheitslücken der gemäss Applikationsliste installierten Soft- oder Hardware und behebt diese umgehend mittels Installation der notwendigen Updates. Wird der Lieferant durch das BBL auf bestehende Sicherheitslückenaufmerksam gemacht, die er noch nicht identifiziert hat, so behebt er diese ebenfalls umgehend durch die Installation eines Updates.

4.4.10 Regelmässige Updates der installierten Software

Unabhängig von gemeldeten Sicherheitslücken, werden mindestens einmal im Jahr alle installierten Tools und Geräte auf die neueste Version upgedatet.

4.4.11 Erstellen eines regelmässigen Abbilds (dump) von Datenbanken

Verfügt die installierte Fachapplikation über eine Datenbank, muss durch den Lieferanten sichergestellt sein, dass diese nach einem Fehler wiederhergestellt werden kann. Dafür soll in regelmässigen Abständen (mindestens einmal Täglich) ein Abbild der Datenbank erstellt und auf der VM der Fachapplikation gesichert werden. Im Fehlerfall wird mit diesem Abbild die Datenbank wiederhergestellt.

5 Managementebene ZUKO-System

5.1 Aufbau

Die Managementebene besteht aus einem Produktiv- und einem Testsystem. Das Produktivsystem beinhaltet die aktuelle Datenbank und steht den Nutzern 24/7 zur Verfügung.

5.2 Funktionalitäten

5.2.1 Mandantenfähigkeit

Die Managementebene muss mandantenfähig sein.
Ist eine Software mandantenfähig, können mehrere Mandanten (Nutzergruppen) gleichzeitig auf demselben Server- oder Softwaresystem verwaltet werden. Dies bedeutet, dass jede Organisationseinheit wie beispielsweise ein Amt, welches die Software benutzt, auf dieselbe Software zugreift, dabei aber eine eigene Oberfläche nutzt sowie individuelle Daten hinterlegen kann, jedoch keinen Zugriff auf andere Mandanten hat und auch keine Daten anderer Mandanten einsehen kann

5.2.2 Benutzerverwaltung

Die folgenden Rollen sollen Zugriff auf die ZUKO-Applikation haben und die Zutrittsberechtigung einsehen und/ oder steuern können:
- Mandanten Administratoren ggfs. mandantenübergreifend
- Hauptadministratoren, welche auch globale (mandantenübergreifende) Konfigurationen vornehmen können
- User des Auftragnehmers (ZUKO-Lieferanten)
- Nur Leserecht: Kann das ganze System einsehen aber nichts verändern. (Für Betrieb IKT-Domotik)
- Weitere nutzerspezifische Anforderungen für die Einsicht und Zutrittsberechtigungen, werden im Betriebshandbuch des Systems detailliert beschrieben.

5.2.3 Anbindung an Datenbezugspunkt Bund

Personendaten müssen über eine Lightweight Directory Access Protocol mit SSL (LDAPS)-Schnittstelle in das System importiert und um Freifelder ergänzt werden können.
Beim Import der Personenstammdaten müssen die Zutrittsmedien für abgelaufene Nutzer (Austrittsdatum) automatisch gesperrt werden und der Personendatensatz nach Ablauf von 90 Tagen ab Sperrdatum gelöscht werden.

5.2.4 Berechtigungskonzept für Mandantenadministratoren

Die Ansicht und Bedienungsmöglichkeiten müssen granuliert eingrenzbar sein, sodass jedem Mandanten Administrator nur jene Funktionen zur Verfügung stehen, welche für seine Arbeit notwendig sind. Die Systemkonfiguration erfolgt gemäss den Vorgaben der Mandantenadministratoren unter Berücksichtigung der technischen Möglichkeiten des Systems.

5.2.5 Objektverwaltung

Objekte (z.B. Türen, Leser, Terminals) und Standorte müssen verwaltet werden können. Die Zuweisung zu den Mandanten muss veränderbar sein.
- Objekte und Standorte müssen in Gruppen, in mehreren Ebenen zusammengefasst werden können.
- Neben den Objekten, die mit der Managementebene verbunden sind (online), existieren an einzelnen Standorten lokale Stand Alone Komponenten (offline). Auch diese Offline-Komponenten müssen in der ZUKO-Applikation erfasst und mit eindeutigen Adressen versehen werden. Diese dürfen kein Subsystem sein.
- Eine hardwarebezogene Zeitsteuerung muss möglich sein. Bspw. muss festgelegt werden können, dass die PIN-Eingabe ausserhalb der Geschäftszeiten bei Lesern mit PIN-Eingabemöglichkeit notwendig ist.

5.2.6 Zutrittsberechtigungsverwaltung

Die Zutritte für Personen / Zutrittsmedien durch die Mandanten Administratoren müssen fein granular (für jedes einzelne Objekt) verwaltet werden können.

- Eine Mischung aus Online- und Offline-Komponenten muss möglich sein.
- Eine Smartcard bezogene Zeitsteuerung muss möglich sein. Bspw. muss festgelegt werden können, dass der Zutritt nur während den Geschäftszeiten möglich ist.
- Eine Kalenderverwaltung, insbesondere für die Berücksichtigung von Feiertagen, muss enthalten sein und bei der Zutrittsberechtigung berücksichtigt werden. Die Kalenderdauer muss mindestens ein Jahr betragen. Die Handhabung wird im Benutzerhandbuch definiert und beschrieben.

5.2.7 Protokollierung

Sämtliche Bewegungen (berechtigte und abgewiesene Zutritte / Zutrittsversuche, Mutationen, Zuweisungen etc.), müssen protokolliert und aufgezeichnet werden. Für die Protokollierung müssen Such- und Filterfunktionen verfügbar sein. Die Datenhistorie der letzten zwei Jahre muss jederzeit abrufbar sein. Daten welche älter sind, sollen automatisch gelöscht werden.

5.2.8 Systemsprachen

Die Sprache der Bedienoberfläche muss einstellbar sein

- Deutsch-Schweiz (DE-ch)
- Französisch (FR-ch)
- Italienisch (IT-ch)
- Englisch (EN-us)

5.2.9 Reporting

Es werden vordefinierte und anpassbare Abfragen für Reporting Zwecke benötigt. Diese müssen mit Export-Funktionen in die gängigen Office-Formate (Excel, Word, PDF) exportiert werden können.

5.2.10 Testumgebung

Um Auswirkungen von Updates und Softwareanpassungen vor der Produktivschaltung testen zu können, wird für jeden ZUKO-Campus ein zweites, mit dem Produktivsystem identisches Testsystem betrieben. Das Testsystem ist nicht mit den Controllern in den Gebäuden verbunden. Es kann bei Bedarf mit Hardwarekomponenten (zu Testzwecken) verbunden werden, welche aber nicht aktiv genutzt werden. Das Testsystem steht primär dem ZUKO-Lieferanten zur Verfügung. Nutzer haben ausschliesslich auf das Produktivsystem Zugriff.

5.3 Bedienung

Nutzer greifen mit physischen Hardware-Clients via einer Virtual Desktop Infrastructure (VDI) über Web-Clients auf die ZUKO-Applikation des Produktivsystems zu, um so die Zutrittsprofile der Personen an den Objekten ihrer Organisationseinheiten dezentral verwalten zu können. Die virtuellen Bedienclients werden von der TGM-Domotik bereitgestellt.

Für Neuinstallationen von ZUKO-Campussystemen gilt, dass die Bedienung der Fachanwendungen über den Bedienclient komplett und ausschliesslich via WEB, mit einem Standard WEB Browser bedient werden können. Dies ohne, dass auf der Clientseite irgendwelche Softwareinstallationen nötig sind, um die Web-Applikationen zu starten oder zu verwenden.

Bei Bestandes-Systemen erfolgt die Bedienung ebenfalls möglichst via WEB-Applikation. Wo dies noch nicht möglich ist, installiert der ZUKO-Lieferant die nötigen Softwareelemente auf einem virtuellen Client, der von der TGM-Domotik zur Verfügung gestellt wird. Dieser dient dann als Mutterclient (Golden Master), für die Erstellung der Nutzerclients.

5.3.1 Mehrbenutzersystem

Die ZUKO-Applikation muss Multiuser-fähig sein. Dies bedeutet, dass mehrere Benutzer mit nicht-persistenten Web-Clients die ZUKO-Applikation gleichzeitig parallel nutzen können.

5.4 Systemanforderungen

Für alle Fachapplikationen werden durch die TGM-Domotik virtuelle Maschinen mit Windows Server Betriebssystem zur Verfügung gestellt und bzgl. Patching, Updates und Upgrades gemanaged. Die TGM-Domotik verwendet als Datenbanksystem (DBS) Microsoft SQL Server und betreibt die Bereitstellung, Verwaltung und tägliche Sicherung der Datenbanken.
Die ZUKO-Applikation muss folgende Kompatibilitäten aufweisen:

- Installation und Betrieb auf Windows Server Systemen, welche regelmässig und automatisiert mit aktuellen Sicherheitsupdates versorgt werden.
- Webserver müssen Transport Layer Security (TLS) 1.2 und höher zertifizierbar sein. Der ZUKO-Lieferant muss den Webserver selbst installieren und die nötigen Zertifikate liefern.
- Datensicherungen müssen jederzeit möglich sein und ohne Betriebsunterbruch erfolgen (siehe Kapitel 4.4.11).

Weitere Eigenschaften der ZUKO-Applikation sind:

- Die ZUKO-Applikation muss ohne direkte Internet-Verbindung betreib- und verwaltbar sein (autark, On-Premises).
- Kabelgebunden: Die ZUKO-Applikation muss ohne Wireless-Kommunikation (WLAN / Mobilfunknetz o.Ä.) betreib- und verwaltbar sein.
- Skalierbar: Die ZUKO-Applikation muss technisch ausbaufähig sein. Dies bezieht sich auf Speicher, Leistung, Datendurchsatz etc.
- Always-on: Die ZUKO-Applikation muss 24/7 verfügbar sein. Downtimes (z.B. zum Einspielen von Updates) müssen planbar sein und dürfen 12 Stunden nicht überschreiten.
- Einfache Replikation: Eine Replikation des Produktiv- in das Testsystem muss stets möglich sein und innerhalb eines Tages abgeschlossen sein.
- Kompatibel zu ZUKO-Hardware: Die Rückwärtskompatibilität zu der eingesetzten ZUKO-Hardware (Automations- und Feldebene) muss während dem Betrieb (mind. 10 Jahre) sichergestellt sein.

5.5 Lizenzierung

Die Lizenzen für die ZUKO-Applikationen sollen nach Möglichkeit als Softwarelösung implementiert werden. Sind Hardware-Lizenzmedien zwingend notwendig, muss der Einsatz und die Montage der nötigen Komponenten mit der TGM-Domotik abgesprochen und koordiniert werden.
Die Lizenzierung der Fachanwendung darf bei einem Restore der virtuellen ZUKO-Server nicht verloren gehen.

5.6 Fernzugriff und Support

Der ZUKO-Lieferant kann ausschliesslich über einen gesicherten VPN-Zugang, welcher vom BIT betrieben wird, auf die Systeme der ZUKO-Applikation zugreifen. Dies gilt sowohl für die initiale Installation wie auch den Support im Betrieb. Die ZUKO-Applikation muss während der gesamten Betriebsphase mit Patches, Updates und Upgrades versorgt werden, um die Verfügbarkeit der Prozesse zu gewährleisten. Dabei darf das Produktivsystem nur nach dem erfolgreichen Testen auf dem Testsystem und einer Freigabe durch die TGM-Domotik aktualisiert werden.
Technische und regulatorische Rahmenbedingungen des Fernzugriffs sind:

- Der Fernzugriff erfolgt ausschliesslich via WEB-Browser auf die VDIs.
- Der VPN-Zugang inkl. der Userverwaltung, wird von der TGM-Domotik gestellt.
- Zur Nachvollziehbarkeit sind ausschliesslich persönliche Benutzerkonten erlaubt.
- Voraussetzung für jeden Mitarbeitenden ist die Unterzeichnung des Dokuments zur Sorgfaltspflicht. Personalmutationen müssen dem BBL umgehend gemeldet werden.

- Falls benötigt, kann ein File Server zur Datenablage/Datenaustausch durch die TGM-Domotik zur Verfügung gestellt werden (Windows Share, SFTP).

5.6.1 Datentransfer

Der Ein- und ausgehende Transfer von Daten zu den ZUKO-Servern erfolgt ausschliesslich via SFTP-Server, welcher von der TGM-Domotik bereitgestellt wird. Ein direkter Zugriff auf die Server ist ausgeschlossen.

5.6.2 Sorgfaltspflichtserklärung

Sämtliche Personen ausserhalb der Bundesverwaltung, insbesondere alle Mitarbeitenden der ZUKO-Lieferanten, welche Zugriff auf die Systeme benötigen, müssen eine schriftliche Sorgfaltspflichterklärung unterzeichnen. Das entsprechende Formular ist bei der TGM-Domotik auf Anfrage erhältlich.

6 Automationsebene ZUKO-System

6.1 Allgemein

Als Automationsebene wird die ZUKO-Hardware für die Zutrittssteuerung in den Gebäuden bezeichnet und beinhaltet alle dafür notwendigen Geräte vor Ort.
Die Controller sind über das Netzwerk der Bundesverwaltung mit der Managementebene verbunden. Profile und Berechtigungen des ZUKO-Systems müssen lokal in den Türcontrollern gespeichert werden. Die Funktion des Systems ist damit auch gegeben, wenn keine Datenverbindung mit dem zentralen Server (Managementebene) besteht. Sollte die Kommunikationsverbindung von der Management- zur Automationsebene unterbrochen sein, muss die elektronische Zutrittskontrollanlage im Gebäude vollumfänglich weiter funktionieren. Alle Ereignisse wie z.B. Buchungen, Türöffnungen und Störungen sollen zwischengespeichert und nach Behebung des Kommunikationsunterbruchs ohne manuellen Eingriff an die Managementebene übertragen werden. Weiter sollen allfällige Mutationen an der Managementebene nach Behebung des Kommunikationsunterbruchs mit der Automationsebene synchronisiert werden.
Generell ist für die Zutrittskontrollanlage sowie für Elektroschlösser, Türöffner etc. keine lokale unterbrechungsfreie Stromversorgung (USV) vorgesehen. Bei einem örtlichen Stromausfall steht die Zutrittskontrollanlage nicht zur Verfügung. Die Türen können während diesem ausserordentlichen Zustand jedoch mechanisch mittels berechtigter Schlüssel geöffnet werden (Intervention).

6.2 Adressierungskonzept

Bei den Systemen im Bestand besteht kein einheitliches Adressierungskonzept für die Automationsebene. Für neue Objekte und bei Sanierungen von ganzen Gebäuden gilt generell das nachfolgende Konzept. Abweichungen von diesem Konzept sind nur nach Rücksprache mit der TGM-Domotik zulässig.

Beispiel **Durchgang**:

Zukunftstrasse 44 in Biel, Raum 312 mit dem Namen Atrium 1 im ersten Untergeschoss ergibt den Namen BIEZUK44_-1.312.T1_Atrium1

Lfd. Nr.	Bezeichnung	Zeichen	Beispiel
1.	Ortschaft	Die ersten 3 Buchstaben	Biel = BIE
2.	Strasse	Die ersten 3 Buchstaben	Zukunftstrasse = ZUK
3	Strassennummer	Komplette Strassennummer	44 = 44
4	Trennzeichen	«Underscore Charakter»	_
5	Stockwerk	bei Untergeschossen wird ein «Minus»-Zeichen verwendet, ansonsten nicht	Untergeschoss 1 = -1
6	Trennzeichen	«Punkt»	.
7	Raumnummer und Türnummer	Falls vorhanden, sonst weglassen	Raumnummer 312 = 312 Türnummer 1 = T1
8	Trennzeichen	«Underscore Charakter»	_
9	Bezeichnung eines Raumes	z. B. Meetingraum, Aula, etc.	Atrium 1 = Atrium1

Controller

Lfd. Nr.	Bezeichnung	Zeichen	Beispiel
1.	Ortschaft	Die ersten 3 Buchstaben	Biel = BIE
2.	Strasse	Die ersten 3 Buchstaben	Zukunftstrasse = ZUK
3	Strassennummer	Komplette Strassennummer	44 = 44
4	Trennzeichen	«Underscore Charakter»	_
5	Stockwerk	bei Untergeschossen wird ein «Minus»-Zeichen verwendet, ansonsten nicht	Untergeschoss 1 = -1
6	Trennzeichen	«Punkt»	.
7	Raumnummer	Falls vorhanden, sonst weglassen	Raumnummer 312 = 312
8	Trennzeichen	«Underscore Charakter»	_
9	Typ und Nummer	AML, AMC etc. die Nummer kommt aus dem Schema	AML05

6.3 Schnittstelle Automationsebene zur Managementebene

Die Netzwerkanbindungen erfolgen ausschliesslich als drahtgebundene LAN-Verbindungen. Anforderungen und Beschrieb sind dem Kapitel 4 «IKT-Bestimmungen» zu entnehmen.

6.4 Anbindungen Feldebene

Für die Anbindung der Feldebene (Sensoren, Aktoren) an die Controller der Automationsebene, sind grundsätzlich nur drahtgebundene Verbindungen zulässig (z.B. Leser). **Wireless Anbindungen sind grundsätzlich nicht zugelassen.** Sofern eine Wireless Anbindung aus technischen oder baulichen Gründen notwendig ist, muss diese durch die TGM-Domotik genehmigt werden.

6.5 Hardware

6.5.1 Technische Grundlagen

Notstromversorgung / USV / Akkus sind nicht Standard und werden durch das BBL nur bei Bedarf eingesetzt.
Der Standort der Controller ist immer auf der sicheren Innenseite des Abschlusses. Dessen Überwachung erfolgt über die Einbruchmeldeanlage.
Admin/Standart-Passwörter in den Controllern müssen durch den Anbieter auf ein sicheres Passwort geändert werden.

Es muss ausschliesslich die LEGIC Advant Technologie verwendet werden (RFID 13.56 MHZ). Trotz des Cross Standard Transponder Chip (CTC) darf die LEGIC prime Technologie zu keinem Zeitpunkt benutzt werden. Zudem ist die Verwendung der UID im Zusammenhang mit der ZUKO nicht zulässig.
Mit der ZUKO-Applikation muss die Segmenteinstellung der Leser online über das Netzwerk einstellbar sein.

Die Kommunikation zwischen Leser und dem ZUKO-Controller oder dem Türcontroller muss über ein verschlüsseltes Protokoll erfolgen.
Leser im Aussenbereich müssen gegen Sabotage überwacht sein.

Bei Spannungsausfall an der Automationsebene muss gewährleistet sein, dass die gesamte Software, alle Daten und die Einstellwerte, erhalten bleiben (Daten- und Programmschutz). Nach Spannungswiederkehr müssen die Automationsebene und die Feldebene automatisch starten und die Betriebsart wie vor dem Ausfall, ohne manuellen Eingriff, wieder aufnehmen. Dies gilt auch für die Verbindung zum Server und die Synchronisation.

Die Immobilienstandorte befinden sich verteilt über die ganze Schweiz und in verschiedenen Höhenlagen. Die Bauteile und Apparate müssen entsprechend den örtlichen klimatischen Verhältnissen standhalten und jederzeit zu 100% funktionieren. Witterungsbedingungen wie Regen, Eis, Schnee, Wind, Sonne, Nebel, Kälte und Hitze dürfen die Funktion nicht beeinträchtigen.

6.5.2 ZUKO-Controller

ZUKO-Controller kommunizieren via LAN-Verbindung mit der Managementebene und drahtgebunden (LAN oder RS-485) mit einem allenfalls vorhandenen Türcontroller.

Die Tür-Controller übernehmen die Auswertungs- und Steuerungsaufgaben der Sensoren (z.B. Leser, Magnetkontakte usw.) und Aktoren (z.B. Türöffner, Motorschlösser usw.). Die Sensoren und Aktoren werden drahtgebunden an die Controller angeschlossen.

Jegliche Controller müssen für Instandhaltungszwecke einfach zugänglich sein. Üblicherweise wird der Zugriff auf den Controller durch die Installation in einem verschlossenen

Raum, Technikschrank oder Steigzone bzw. durch eine Montage in erhöhter Position eingeschränkt. Die an den Controller angeschlossenen Kabel müssen eindeutig beschriftet sein (z. B. „Leser innen“, „Rahmenkontakt Stehflügel“).

6.5.3 Online-Leser

Alle Leser sind ausgelegt, um segmentierte Chips mit einer Frequenz von 13,56 MHz auszulesen. Um die Systemintegration zu gewährleisten, ist die Chiptechnologie LEGIC Advant anzuwenden (ISO 14443 A).
Die Auslesung erfolgt berührungslos und verschlüsselt mit Triple Data Encryption Standard (3DES) und/oder Advanced Encryption Standard (AES). Die Lesedistanzen betragen zwischen 2cm und 10cm.

Die Online-Leser müssen für folgende Segmente konfiguriert sein (Erweiterungen und Neubau):
- BBL Legic Access Segment (FB 3A 0A 12 01)
- BBL Legic Übergangssegment (FB 3A 0A 02 40)
- BBL Legic ZUKO Segment (FB 3A 0A 00) ist noch bis **31.12.2027** zugelassen. Anschliessend dürfen nur noch die obenstehenden beiden Legic Segmente verwendet werden.

Leser, welche biometrische Daten nutzen, sind generell nicht zugelassen.

6.5.4 Offline-Komponenten

Offline-Leser und Offline-Komponenten sind nur in Ausnahmefällen, in Absprache mit der TGM-Domotik erlaubt.

Die Offline-Komponenten müssen für folgendes Segment konfiguriert sein:
- BBL Legic OSS SO Segment (FB 3A 0A 05 10)
- BBL Legic OSS SID Segment (FB 3A 0A 05 20)

6.5.5 Validierungsleser

Das Benützen von Validierungslesern soll für den Nutzer eine bewusste Handlung sein. Somit werden Validierungsleser nicht mit einem Zutrittsleser kombiniert. Die Validierungsleser sollen an einem sinnvollen Standort montiert werden, z. B. neben dem Zeiterfassungsterminal. Die Validierungszeit soll möglichst kurz eingestellt sein. Die Empfehlung ist 24h.

6.5.6 SAM-Karten (Taufkarten zu Offline-Komponenten)

SAM – Karten werden zum Taufen von Validierungsleser oder Offline – Komponenten benötigt. Die SAM – Karten sind Eigentum von TGM-Domotik. Die SAM – Karten können bei Bedarf vom ZUKO-Lieferanten bei der TGM-Domotik angefordert werden (Vorlaufzeit 3 Wochen).

6.5.7 Programmer zu Offline-Komponenten

Programmiergeräte für die Programmierung von Offline-Komponenten müssen sich vor Ort im betroffenen Objekt befinden, inkl. allfällig benötigten Masterkarten. Für die Programmiergeräte und die dazu gehören Masterkarten sind die Mandanten Administratoren vor Ort zuständig und verwalten diese Komponenten. Die Schulung der Nutzer erfolgt durch den ZUKO-Lieferanten.

7 Zutrittsmedium

7.1 Allgemein

Als Zutrittsmedium ist die Smartcard des Bundes der Standard. Technologien, welche mit biometrischen Daten arbeiten, sind aus Datenschutzgründen nicht zugelassen. Auf der Smartcard stehen für die ZUKO je 1 Segment für Online- und Offline-Anwendungen zur Verfügung. (Siehe Kap. 6.5.3 und 6.5.4). Abweichungen dazu müssen mit der TGM-Domotik abgesprochen werden.

8 Schulungen

Die Schulung der Benutzer und das Einrichten der Mandanten Administratoren auf dem Managementsystem, erfolgen durch den ZUKO-Lieferanten.

9 Dokumentation

9.1 Betriebshandbuch

Durch den ZUKO-Lieferanten ist in Zusammenarbeit mit der TGM-Domotik ein Betriebshandbuch für die Mandanten Administratoren zu erstellen. Dieses wird den Nutzern auf einem SharePoint des BBL zur Verfügung gestellt.

9.2 Share Point

Das BBL stellt relevante Dokumente und Informationen auf einem SharePoint zur Verfügung.

10 Verfasser und Bezugsquelle

Diese Weisungen wurden durch die Fachberatung PM zusammen mit dem technischen Gebäudemanagement (TGM, OM) erarbeitet und werden bei Bedarf angepasst.

Diese Weisung kann online unter folgendem Link (Kapitel Fachberatung Gebäudetechnik) bezogen werden:

Downloads Bauten

11 Inkraftsetzung

Diese Weisungen treten am 1. Februar 2026 in Kraft.

Bundesamt für Bauten und Logistik

Froesch Martin 3VLPU4
30.01.2026

Info: admin.ch/esignature | validator.ch

Martin Frösch
Bereichsleiter Bauten